09768839 "122700

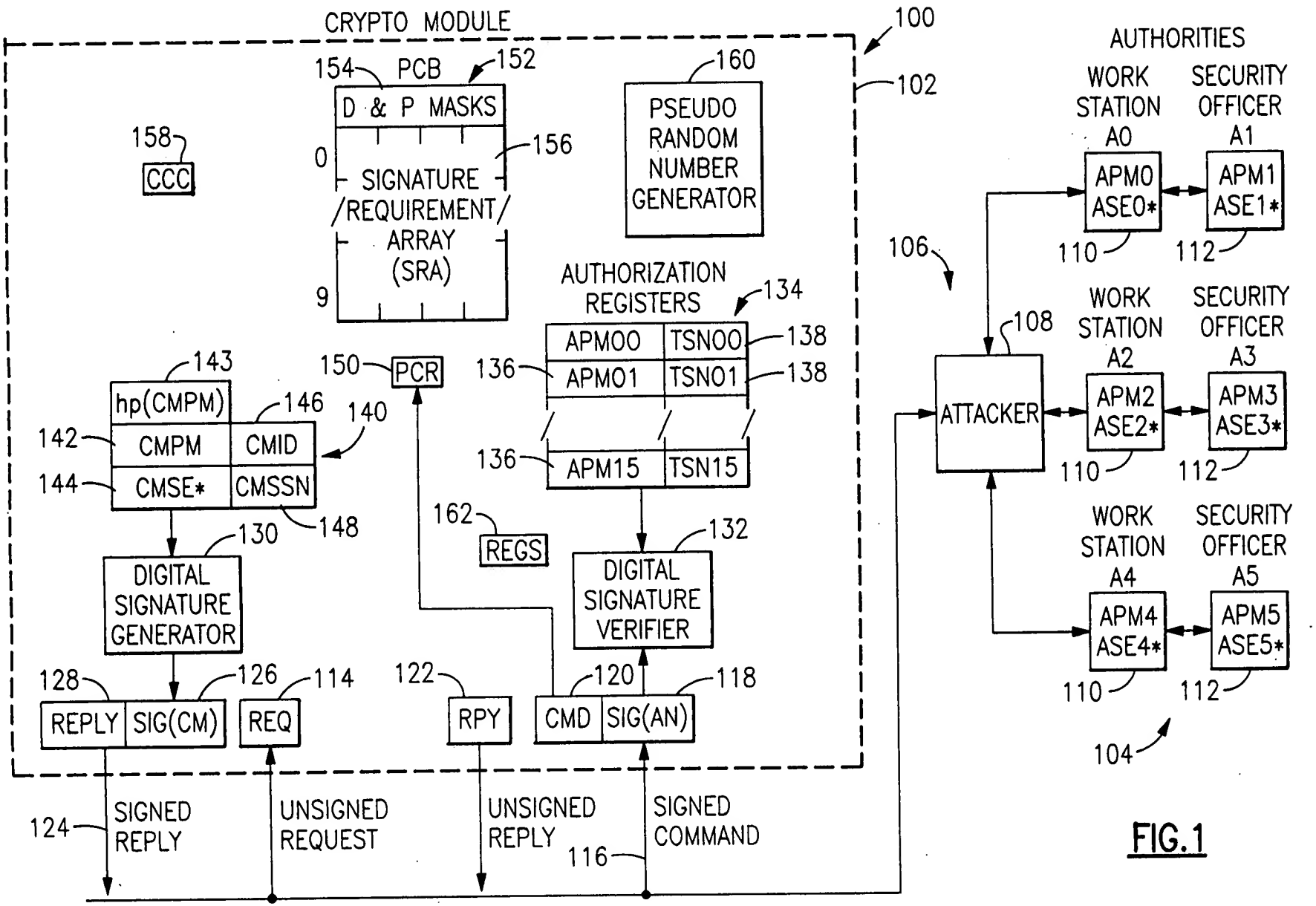

FIG.1

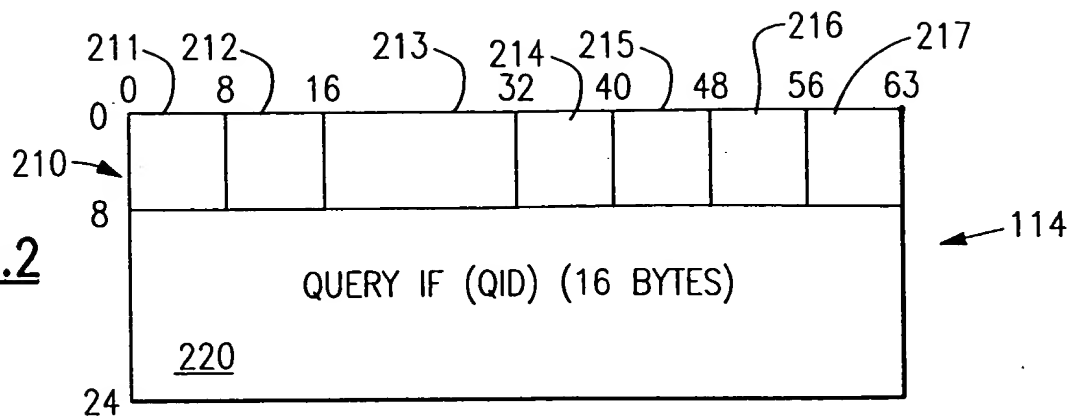
211
212
213
214
215
216
217
0
8
16
32
40
48
56
63
0
210
8
114
QUERY IF (QID) (16 BYTES)
220
24

FIG.2

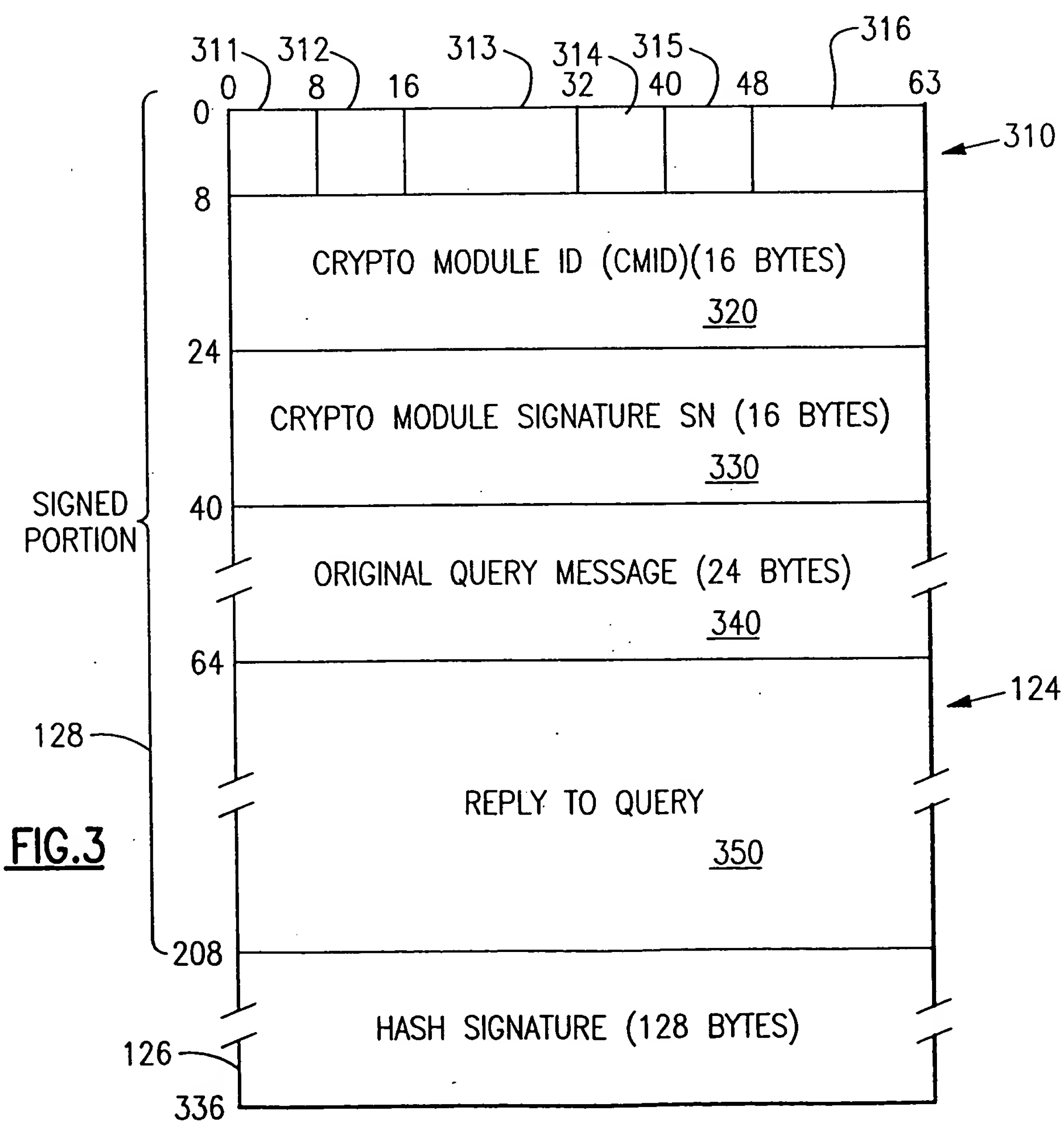
311
312
313
314
315
316
0
8
16
32
40
48
63
0
310
8
CRYPTO MODULE ID (CMID)(16 BYTES)
320
24
CRYPTO MODULE SIGNATURE SN (16 BYTES)
330
SIGNED PORTION
40
ORIGINAL QUERY MESSAGE (24 BYTES)
340
64
124
128
REPLY TO QUERY
350
208
HASH SIGNATURE (128 BYTES)
126
336

FIG.3

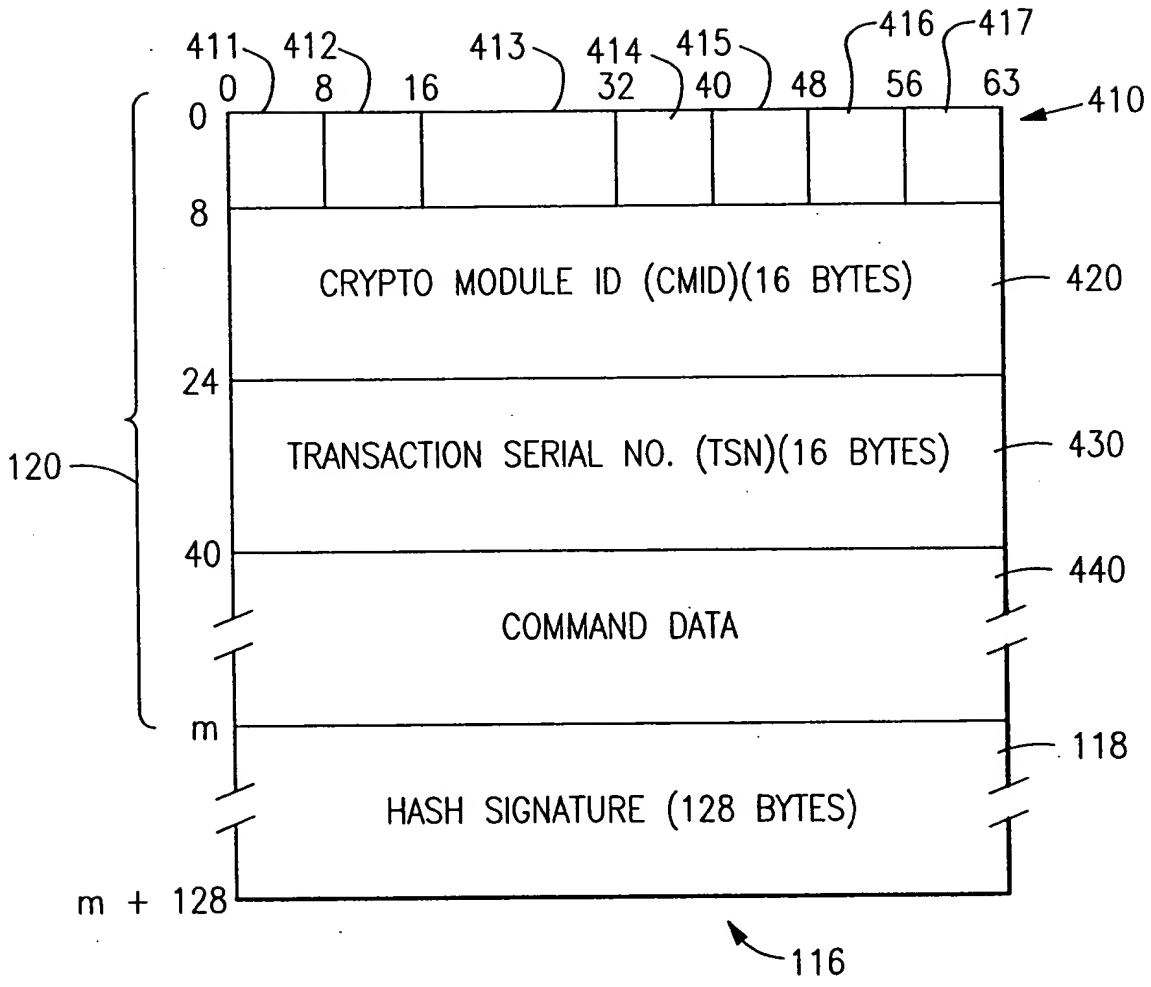
411
412
413
414
415
416
417
0
8
16
32
40
48
56
63
410
0
8
CRYPTO MODULE ID (CMID)(16 BYTES)
420
24
TRANSACTION SERIAL NO. (TSN)(16 BYTES)
430
120
40
440
COMMAND DATA
m
118
HASH SIGNATURE (128 BYTES)
m + 128
116

FIG.4

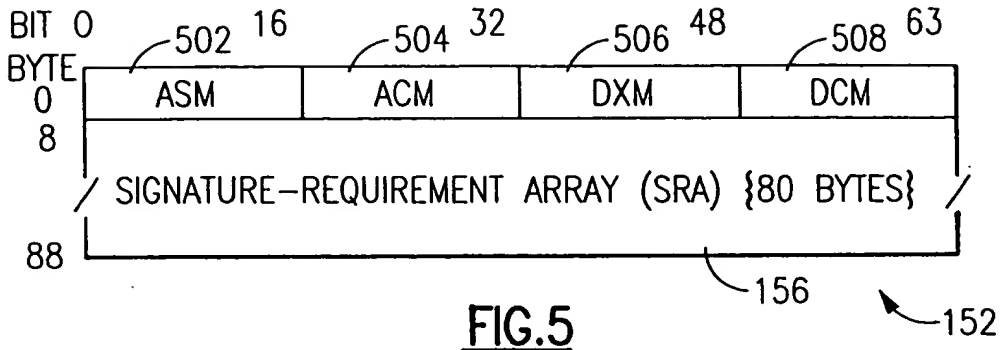

FIG.5

BYTE	SIGNATURE-REQUIREMENT ARRAY (SRA)	156
0	ENTRY 0, FOR LOAD AUTHORIZATION PUBLIC MODULUS (LAP)	602
8	ENTRY 1, FOR LOAD PKSC CONTROL BLOCK (LCB)	602
16	ENTRY 2, FOR ZEROIZE DOMAIN (ZD)	602
24	ENTRY 3, FOR LOAD ENVIRONMENT-CONTROL MASK (LEC)	
32	ENTRY 4, FOR EXTRACT AND ENCRYPT MASTER KEY (XEM)	
40	ENTRY 5, FOR LOAD KEY PART (LKP)	
48	ENTRY 6, FOR EXTRACT AND ENCRYPT SMK OR RMK (XES OR XER)	
56	ENTRY 7, FOR LOAD AND COMBINE SMK OR RMK (LCS OR LCR)	
64	ENTRY 8, FOR REENCIPHER TO SMK OR RMK (RTS OR RTR)	
72	ENTRY 9, FOR REENCIPHER FROM SMK OR RMK (RFS OR RFR)	

FIG.6

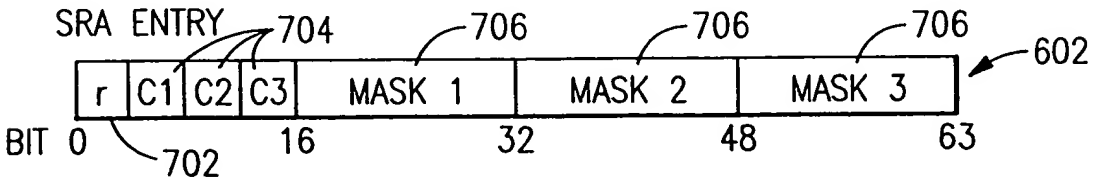

FIG.7

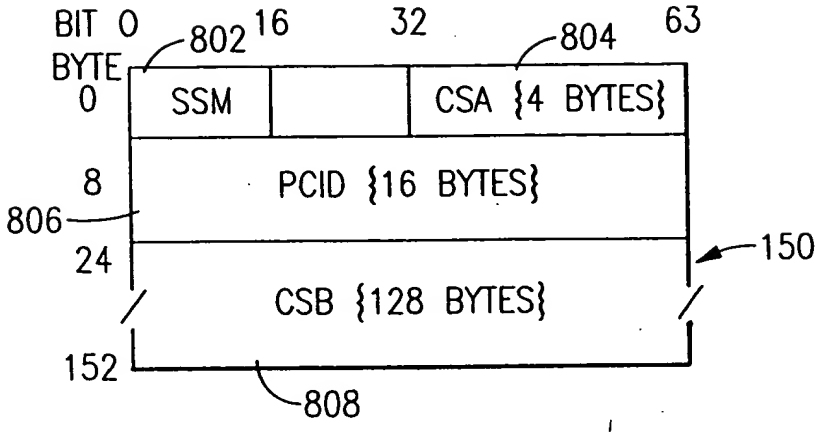
BIT 0
16
32
63
802
804
BYTE
0
SSM
CSA {4 BYTES}
8
PCID {16 BYTES}
806
24
150
CSB {128 BYTES}
152
808

FIG.8

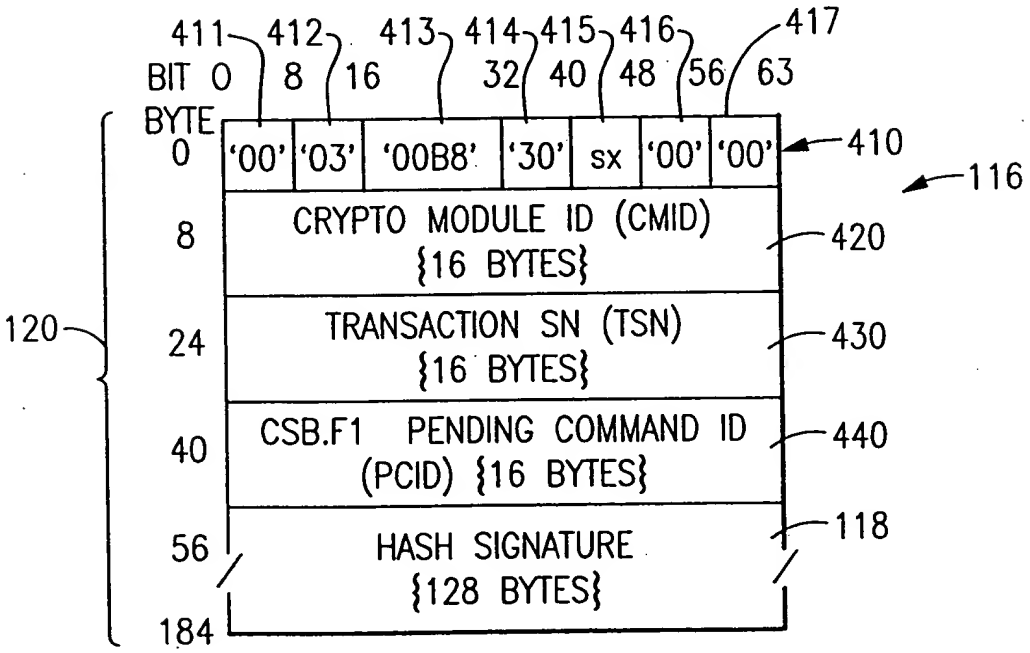
411
412
413
414
415
416
417
BIT 0
8
16
32
40
48
56
63
BYTE
0
'00'
'03'
'00B8'
'30'
sx
'00'
'00'
410
116
8
CRYPTO MODULE ID (CMID) {16 BYTES}
420
120
24
TRANSACTION SN (TSN) {16 BYTES}
430
40
CSB.F1 PENDING COMMAND ID (PCID) {16 BYTES}
440
56
HASH SIGNATURE {128 BYTES}
118
184

FIG.9

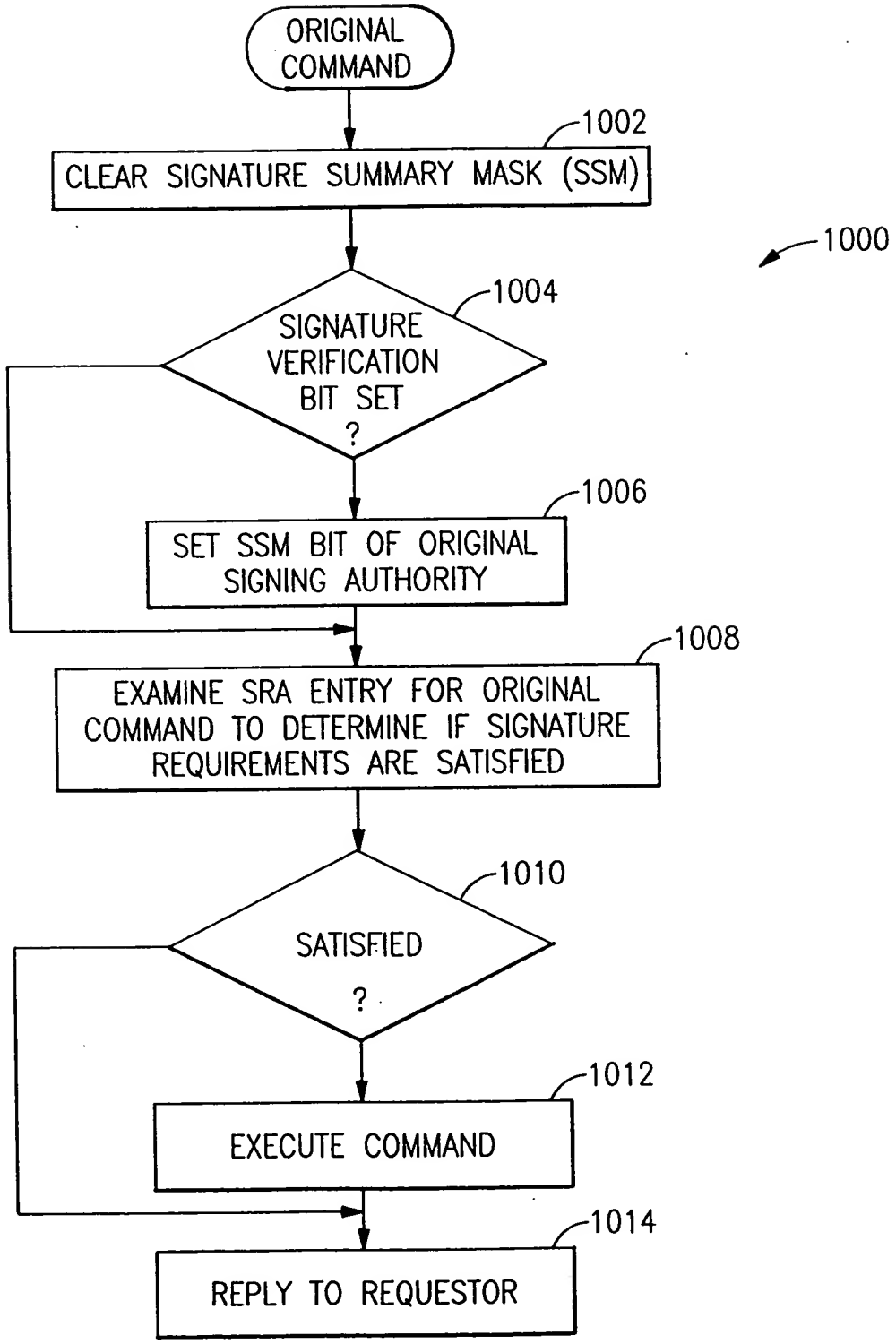
ORIGINAL COMMAND
1002
CLEAR SIGNATURE SUMMARY MASK (SSM)
1000
1004
SIGNATURE VERIFICATION BIT SET ?
1006
SET SSM BIT OF ORIGINAL SIGNING AUTHORITY
1008
EXAMINE SRA ENTRY FOR ORIGINAL COMMAND TO DETERMINE IF SIGNATURE REQUIREMENTS ARE SATISFIED
1010
SATISFIED ?
1012
EXECUTE COMMAND
1014
REPLY TO REQUESTOR

FIG.10

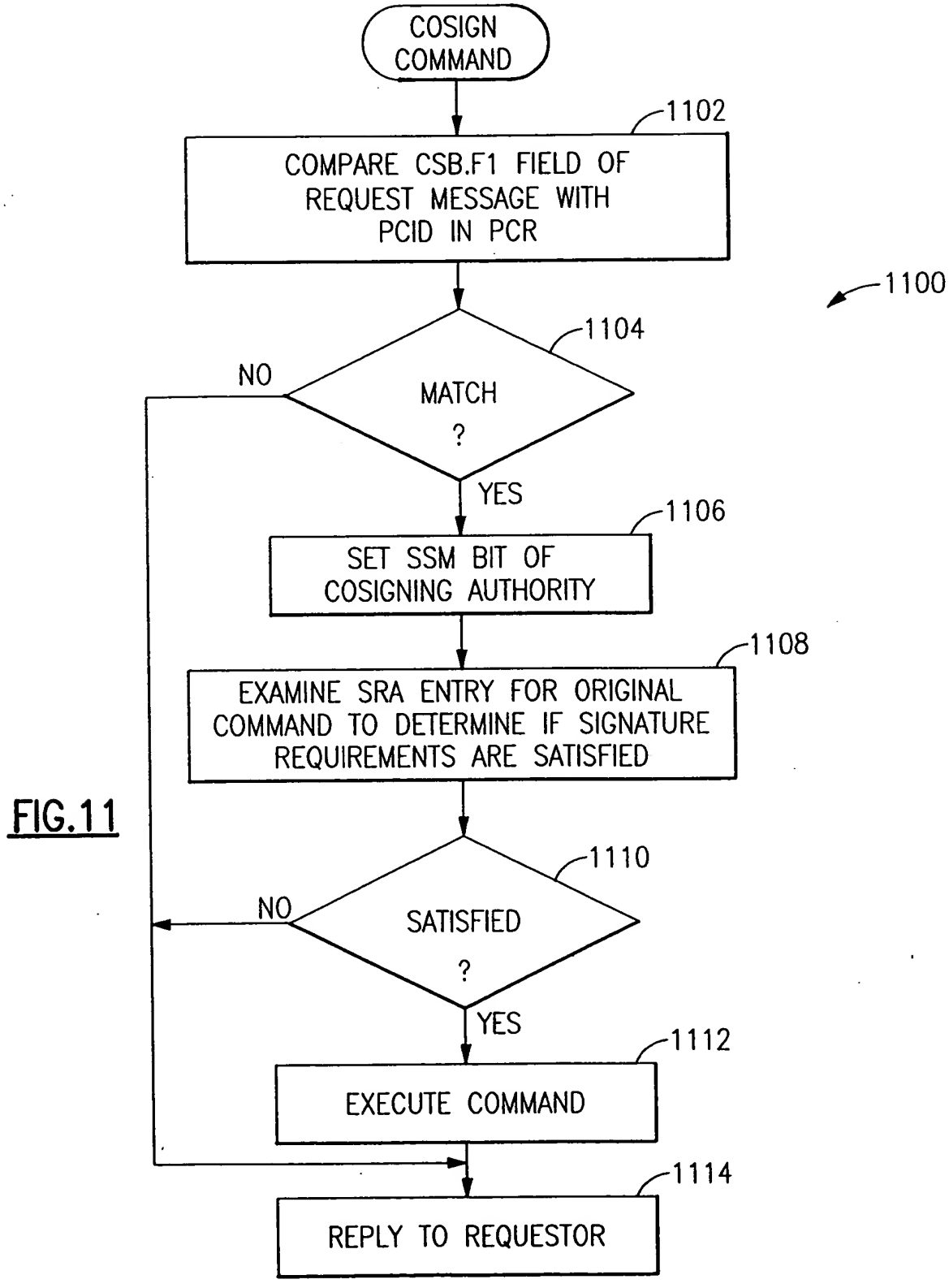
COSIGN COMMAND
1102
COMPARE CSB.F1 FIELD OF REQUEST MESSAGE WITH PCID IN PCR
1100
1104
NO
MATCH ?
YES
1106
SET SSM BIT OF COSIGNING AUTHORITY
1108
EXAMINE SRA ENTRY FOR ORIGINAL COMMAND TO DETERMINE IF SIGNATURE REQUIREMENTS ARE SATISFIED
1110
NO
SATISFIED ?
YES
1112
EXECUTE COMMAND
1114
REPLY TO REQUESTOR

FIG.11

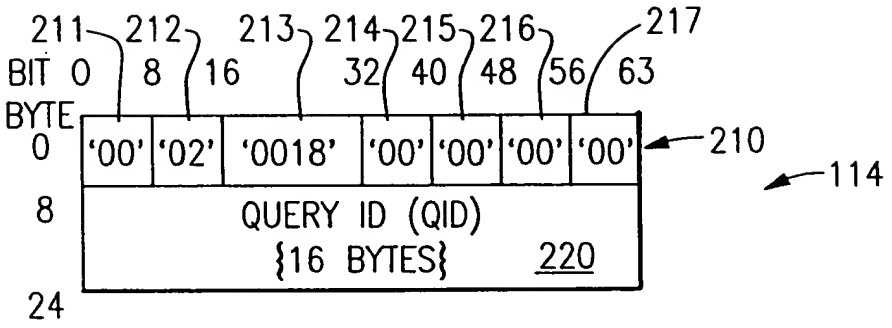
211
212
213
214
215
216
217
BIT 0
8
16
32
40
48
56
63
BYTE
0
'00'
'02'
'0018'
'00'
'00'
'00'
'00'
210
114
8
QUERY ID (QID)
{16 BYTES}
220
24

FIG.12

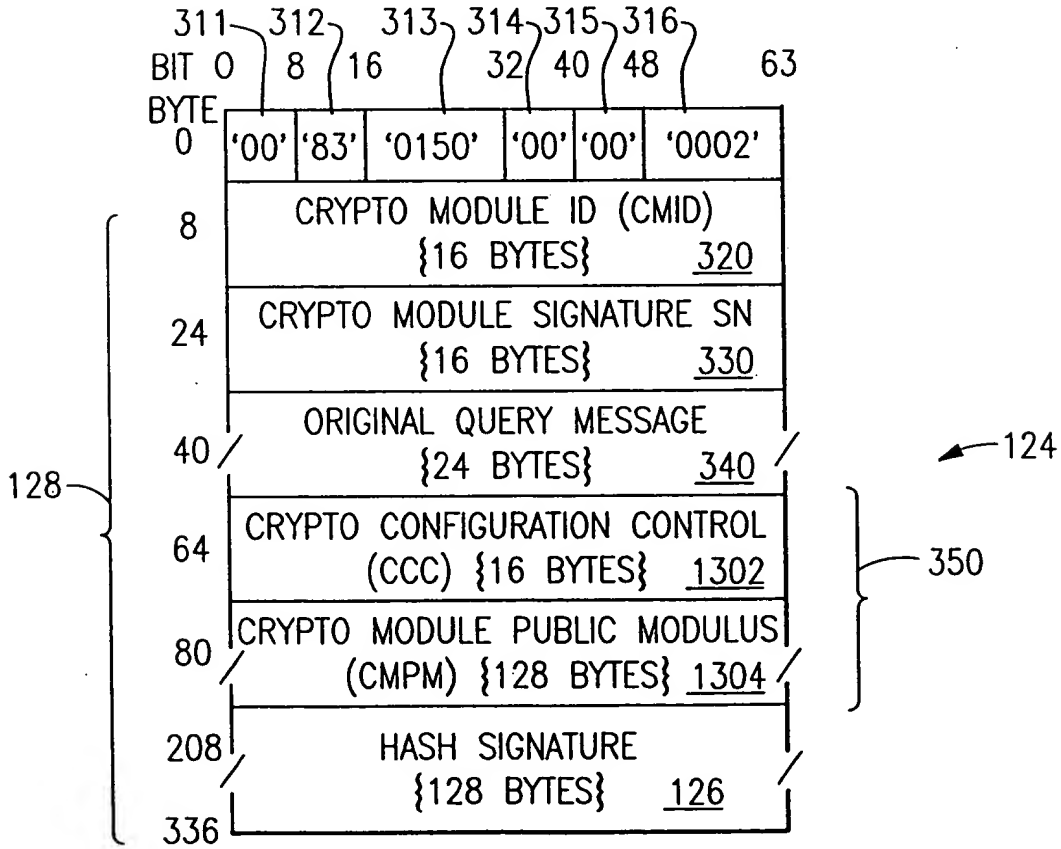
311
312
313
314
315
316
BIT 0
8
16
32
40
48
63
BYTE
0
'00'
'83'
'0150'
'00'
'00'
'0002'
8
CRYPTO MODULE ID (CMID)
{16 BYTES}
320
24
CRYPTO MODULE SIGNATURE SN
{16 BYTES}
330
40
ORIGINAL QUERY MESSAGE
{24 BYTES}
340
124
128
64
CRYPTO CONFIGURATION CONTROL
(CCC) {16 BYTES}
1302
350
80
CRYPTO MODULE PUBLIC MODULUS
(CMPM) {128 BYTES}
1304
208
HASH SIGNATURE
{128 BYTES}
126
336

FIG.13

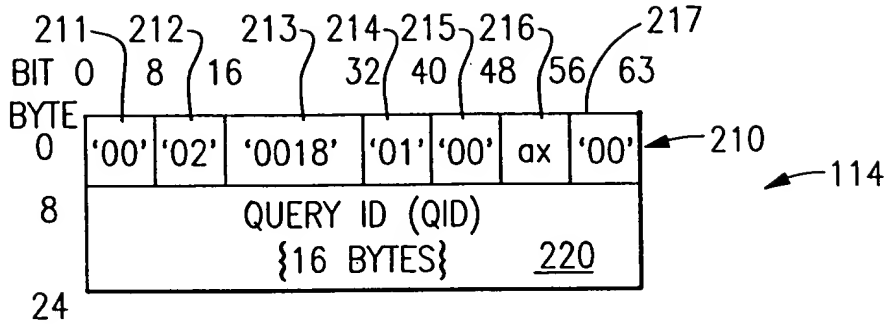
211
212
213
214
215
216
217
BIT 0
8
16
32
40
48
56
63
BYTE
0
'00'
'02'
'0018'
'01'
'00'
ax
'00'
210
114
8
QUERY ID (QID)
{16 BYTES}
220
24

FIG.14

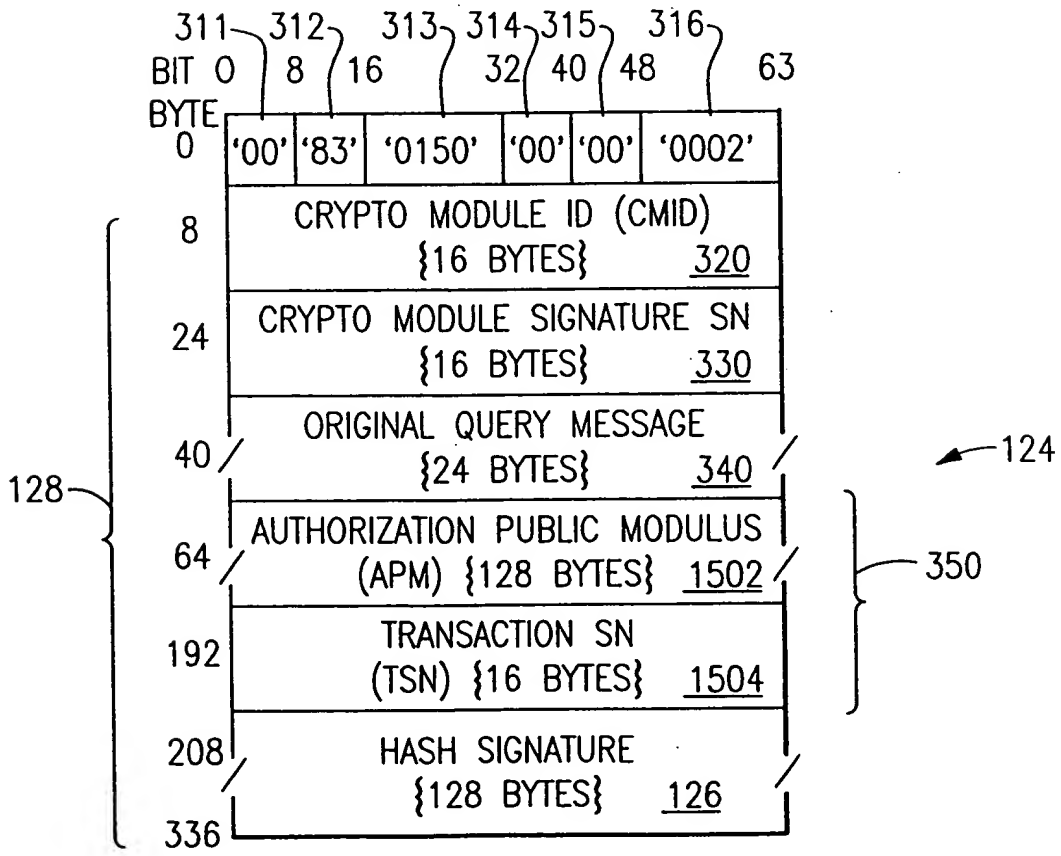
311
312
313
314
315
316
BIT 0
8
16
32
40
48
63
BYTE
0
'00'
'83'
'0150'
'00'
'00'
'0002'
8
CRYPTO MODULE ID (CMID)
{16 BYTES}
320
24
CRYPTO MODULE SIGNATURE SN
{16 BYTES}
330
40
ORIGINAL QUERY MESSAGE
{24 BYTES}
340
124
128
64
AUTHORIZATION PUBLIC MODULUS
(APM) {128 BYTES}
1502
350
192
TRANSACTION SN
(TSN) {16 BYTES}
1504
208
HASH SIGNATURE
{128 BYTES}
126
336

FIG.15

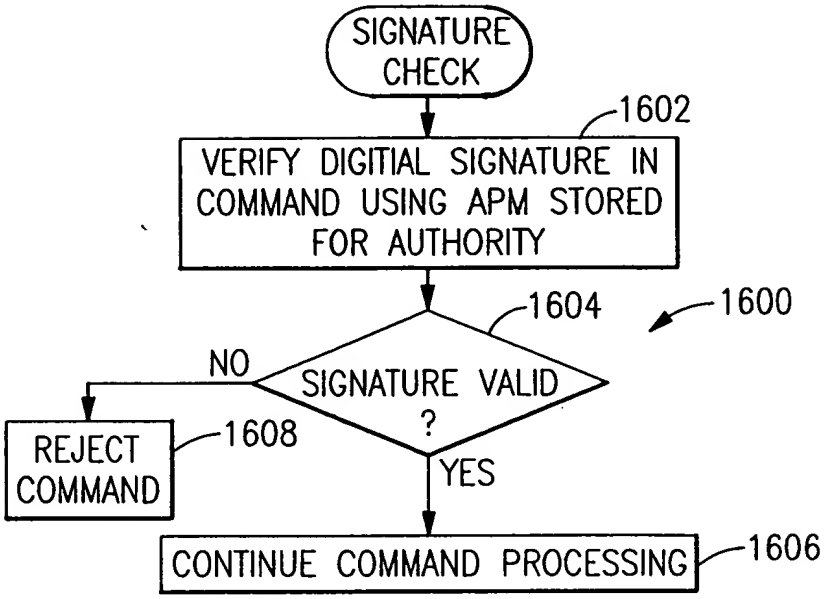

FIG.16

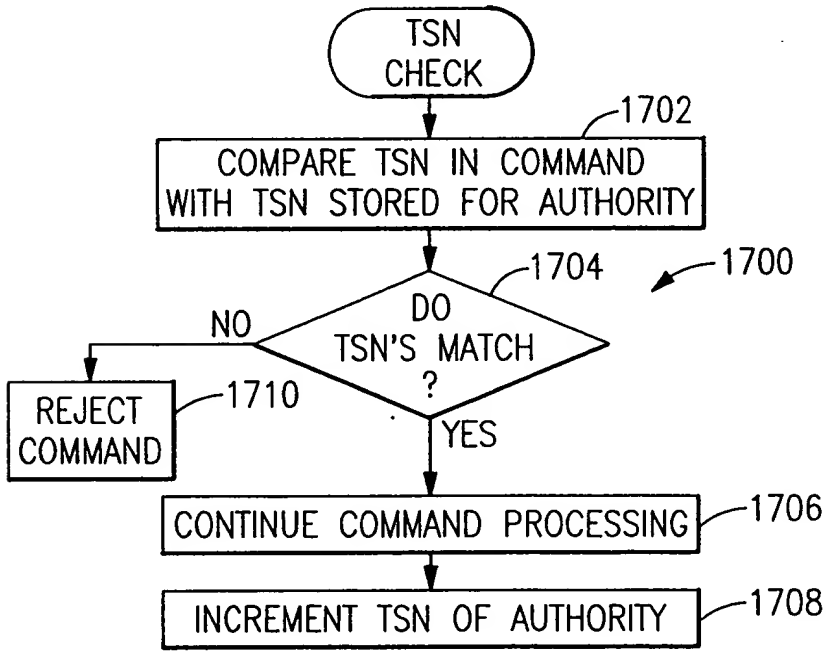

FIG.17

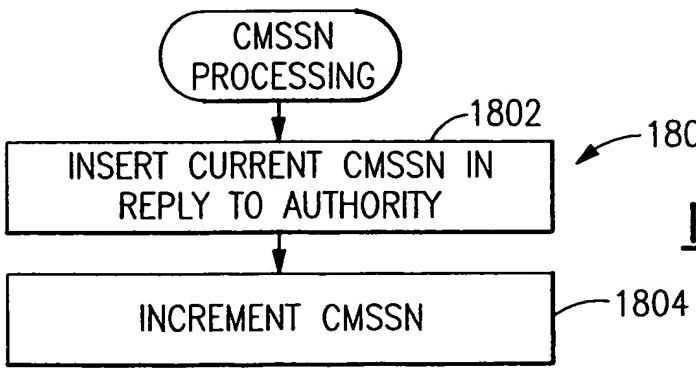

FIG.18

Docket #PO9-97-091